Défis pour la variabilité et la traçabilité des exigences en ingénierie système

Nicolas Sannier, Benoît Baudry

Défis pour la variabilité et la traçabilité des exigences en ingénierie système.

Nicolas Sannier[*,**] **- Benoît Baudry**[*]

***** *EDF R&D, Département STEP, groupe P1A*
6 Quai Watier BP49 78401 Chatou

****** *INRIA Rennes Bretagne-Atlantique*
Campus de Beaulieu 35042 Rennes cedex

nicolas.sannier {@edf.fr @inria.fr}, benoit.baudry {@inria.fr}

RÉSUMÉ : *Les grands projets industriels font face à une volumétrie importante des exigences, souvent contraintes par un cadre réglementaire ou législatif important mais implicite. Ces projets sont menés via des approches centrées documents et connaissent une variabilité importante de leurs exigences tant à la conception que pendant l'exploitation. Après avoir identifié un certain nombre de facteurs de variabilité, nous nous positionnons pour une approche dirigée par les modèles pour expliciter ce contexte réglementaire et adresser la variabilité et la traçabilité des exigences dans un contexte industriel et sûreté de fonctionnement.*

ABSTRACT: *Major industrial projects are facing an important size of their requirements documents, often based on an implicit normative or legislative context. Managed through a document-centric approach, they are facing two challenges: variability and traceability of their requirements at both design time and runtime. In the paper, we identify vectors of variability and propose model-driven engineering as a solution to tame this normative context and address variability and traceability concerns in an industrial context with safety concerns*

MOTS-CLÉS : *exigences, ingénierie dirigée par les modèles, ingénierie des exigences, variabilité, traçabilité, sûreté de fonctionnement*

KEYWORDS: *requirements, model-driven engineering, requirements engineering, variability, traceability, safety*

---

1. Introduction et motivations

La bonne gestion des exigences d'un système est un facteur clé de la réussite d'un projet industriel. Ces exigences sont souvent portées par un cadre normatif voire législatif, contraignant le système dans sa conception et son exploitation durant sa vie. La conformité aux standards, la certification, les organismes de réglementation, les contextes économiques, politiques, historiques, environnementaux sont autant de facteurs impactant un système dans son ensemble, et pour ce qui nous intéresse, les exigences qui définissent ce dernier.

La sûreté de fonctionnement est aujourd'hui primordiale pour les systèmes industriels complexes et pour lesquels, les approches Model-based Systems Engineering sont vues comme des éléments à forte valeur ajoutée. La formalisation des exigences à travers des modèles permet de capitaliser les connaissances, proposer des solutions d'analyse automatique par rapport aux approches centrées sur les documents (et donc leur interprétation subjective) dont la volumétrie explose pour les projets à très longue durée de vie et pour lesquels la variabilité et la traçabilité sont des facteurs clés.

Ce papier vise à identifier des facteurs de variabilité des systèmes et les conséquences sur la description des exigences système d'EDF. Cette analyse nous conduit à établir un ensemble de questions, auxquelles il nous faudra répondre si nous voulons prendre en compte ce contexte document-centré et où la traçabilité est un facteur primordial pour garantir la robustesse des analyses menées à partir de ces modèles. Nous proposons ensuite un état de l'art de la métamodélisation pour l'ingénierie des exigences et identifions des défis majeurs qu'il nous faut relever pour la gestion et l'analyse de la variabilité dans les exigences système d'EDF.

La suite du document est organisée de la façon suivante. Nous décrivons brièvement dans la première partie le contexte de recherche où nous nous trouvons à savoir à la croisée de l'ingénierie des exigences et de l'ingénierie dirigée par les modèles. La section suivante présente le contexte industriel de nos travaux ainsi que les dimensions de variabilités et de traçabilité liées à ce dernier. Les sections 5 et 6 illustrent, à partir de quelques exemples tirés de l'existant, en quoi nous croyons que l'ingénierie dirigée par les modèles peut servir à l'analyse des exigences dans un tel contexte et des premiers éléments de solution pour le challenge qui nous est imposé.

2. L'ingénierie des exigences et l'ingénierie dirigée par les modèles

L'ingénierie des exigences est un processus d'ingénierie qui peut se décrire en plusieurs tâches. Le découpage proposé par (Cheng *et al*, 2008) se traduit par des

étapes d'élucidation, de modélisation, d'analyse, de validation et vérification et enfin de management. Un tour d'horizon du domaine montre que c'est un sujet particulièrement complexe. On se situe dans l'espace de problème, plus ouvert, plus incertain tandis que le génie logiciel est traditionnellement ancré dans l'espace des solutions. C'est un sujet pluridisciplinaire, avec un facteur humain important. C'est un espace instable, sujet à une forte variabilité, en amont des phases de développement et même pendant le développement et l'exploitation. Enfin, il n'y a pas d'approche globale sur le sujet, les travaux se focalisant sur un des aspects cités.

De manière transverse à toutes ces tâches vient également se greffer la problématique de la variabilité et de la traçabilité que nous exprimons au regard du contexte industriel de nos travaux futurs.

L'ingénierie dirigée par les modèles (Jezequel *et al*, 2006) propose un cadre méthodologique et technologique qui permet d'unifier différentes façons de procéder de manière homogène par l'utilisation intensive des modèles. Cette unification entre les modèles, est réalisée à travers la transformation (automatique) pour passer de l'un à l'autre de façon plus souple, plus fiable et de proposer par raffinement successifs d'aller de la conception à l'exécution et de proposer le juste niveau d'abstraction à un moment donné.

Un modèle est une représentation abstraite, incomplète et imparfaite de ce que l'on décide de décrire. C'est encore plus vrai quand on se place dans le cadre de l'ingénierie des exigences. Cependant l'ingénierie dirigée par les modèles offre une solution intéressante à ce contexte instable par nature de par la formalisation à travers le cadre structurel qu'offre le métamodèle, et d'autre part de proposer à travers la transformation de modèles des possibilités d'unifier les activités traitées séparément d'un processus d'ingénierie des exigences et d'améliorer la traçabilité entre étapes.

3. Contexte industriel proposé par EDF R&D

3.1 Variabilité des exigences

EDF possède un parc de 58 tranches de centrales nucléaires. Chaque tranche est considérée comme une entité différente des autres et doit être l'objet d'une démonstration de sûreté chaque dix ans (visite décennale) pour pouvoir être exploitée dix ans de plus. Aujourd'hui, les tranches ont des durées de vie d'au moins quarante ans, sur des périodes reconductibles, validées par l'autorité de sûreté nucléaire. Les incidents, les retours d'expériences obtenus au fil de l'exploitation, ou simplement les évolutions de la société ont amené les autorités à modifier leurs

exigences au fil du temps, amenant les concepteurs/exploitants à devoir démontrer la sûreté sur de nouveaux critères (nouveaux critère de rejets environnementaux par exemple). Au fil des années, le matériel devenu obsolescent est lui aussi remplacé et ce nouveau matériel doit lui aussi être qualifié (temps de réponse, conditions physiques d'utilisation). Nous avons identifié là un premier facteur de variabilité : le temps.

Dans un contexte de renouveau du nucléaire à l'international, cela implique pour EDF d'avoir à faire avec des autorités de sûreté différentes, avec leur fonctionnement, histoire, cadre réglementaire, pratique propre, d'avoir à faire probablement avec de nouveaux partenaires, de vendre des infrastructures clés en main ou de devoir s'adapter à des spécifications nationales... Les documents normatifs internationaux impliquent nécessairement des interprétations qui peuvent différer. Ces interprétations peuvent amener à prouver le système de façon différente, d'allouer une fonction à un système dissocié plutôt qu'à un autre déjà existant, d'utiliser un autre type d'élément (choix de capteurs analogiques vs numériques par exemple). Nous venons d'identifier un second facteur de variabilité : la globalisation.

Gérer un parc de centrales comme en France est différent de gérer une ou plusieurs centrales dans un autre pays. Les modes de fonctionnement sont différents entre un fonctionnement régulier en régime permanent et un fonctionnement qui doit s'adapter au besoin du réseau, en phase d'arrêt ou de redémarrage. Les contraintes sur les éléments sont différentes. De même, un élément possède également une vie, n'est disponible (son bon fonctionnement a été démontré) que pour certains états du système, à certaines conditions physiques (température, pression, pH, …) particulières. Le contexte représente donc un troisième facteur de variabilité.

Ces dimensions se retrouvent non seulement à un haut niveau d'abstraction comme décrit précédemment, mais également à travers tout le système jusque dans ces moindres composants.

3.2 Traçabilité des exigences

(Gotel *et al*, 1994) définissent la traçabilité comme : « *the ability to describe and follow the life of a requirement, in both a forward and backward direction (i.e. from its origin, through its development and specification, to its subsequent deployment and use, and through periods of on-going refinement and iteration in any of these phases)* ». Les grands projets industriels sont sujets à une volumétrie d'exigences extrêmement importante, généralement sous forme textuelle. De plus, les raisons pour lesquelles les exigences sont spécifiées ont un caractère souvent implicite,

limité à une ou quelques personnes possédant une expertise particulière, qui peuvent justifier d'un choix technologique, politique, économique à un moment donné. A l'échelle de la durée de vie d'un projet industriel long (plusieurs années de conception, des décennies d'exploitation), il est vital d'expliciter le lien non seulement entre l'exigence une fois formalisée et sa mise en œuvre concrète mais aussi au niveau abstrait, sur sa justification.

Si on considère la littérature aujourd'hui, on peut s'apercevoir que cette définition est très souvent amputée de sa partie entre parenthèses dans les faits et si les travaux, outils, standards mentionnent les sources, les origines d'une exigence, ils restent à la marge (Yue *et al*, 2010), et les représentent sous la forme d'historique ou de statut (brouillon, soumis, refusé…) ou de sources externes dans les outils de gestion des exigences.

3.3 Bilan

Ces deux aspects, variabilité et traçabilité sont intimement liés. Pour être à même de connaître l'impact d'une modification d'une exigence au cours de la conception, du développement et de l'exploitation d'un système, il faut avoir été capable de la tracer d'un bout à l'autre et dans les deux directions puisque la modification peut provenir :

- De l'allocation : Dans le cas d'un remplacement, il faudra pouvoir remonter aux exigences et démontrer que son remplaçant continue d'y répondre
- De l'exigence en elle-même, par exemple la modification de critères particuliers auquel cas, il faudra vérifier que les éléments impactés par cette exigence continuent d'y répondre.
- De la démarche de qualification mise en œuvre pour vérifier la bonne prise en compte des exigences dans la conception du système proposé. Là où, par exemple, une vérification par simulation était nécessaire, il se peut que pour un contexte donné, il faille plutôt s'orienter par une preuve formelle ou un autre type de démonstration.

4. L'Ingénierie dirigée par les modèles appliquée à l'analyse des exigences

4.1 Questions et approches

Partant des observations synthétisées dans la section précédente, nous nous posons les questions suivantes qui guident nos recherches : Qu'est ce qu'une exigence ? Quels sont les différents types d'exigence ? Quelles sont les relations entre ces exigences et le système, les acteurs ? Comment les représente-t-on ?

Au niveau des exigences, il existe plusieurs catégorisations possibles, correspondant au besoin de description du moment. Si Lamsweerde considère des buts, des « soft goals », des exigences et des attentes, d'autres considèrent le côté fonctionnel, non fonctionnel, ou des décompositions plus fines comme par exemple une décomposition des exigences selon le domaine qu'elles adressent : l'électricité, la mécanique…

Il existe un nombre important de méthodes pour définir, structurer les besoins d'un système parmi les plus célèbres i*, orientée agent (Yu 95) ou encore KAOS, orientée but (Van Lamsweerde, 2009). Ces méthodes cependant ne permettent que de spécifier un ensemble d'exigences pour un système. Elles n'adressent pas la façon dont elles sont suivies, leur évolution ou leur validation au cours de la durée de vie d'un projet. Cependant, elles montrent une bonne expressivité pour montrer les compositions, les relations avec le système d'un point de vue statique en phase de conception. Nous présentons brièvement KAOS et exhibons des propriétés qui nous intéressent par la suite.

4.2 La méthode KAOS

KAOS (Knowledge Analysis in autOmated Specification) résulte des travaux des universités de Louvain et de l'Oregon sous l'impulsion du professeur Axel Van Lamsweerde (Van Lamsweerde, 2009). C'est une approche multivue (modèle de buts, de responsabilité, d'objets, de comportement …) qui permet d'élucider, spécifier, un modèle d'exigences sous une forme structurée et hiérarchique. Dans KAOS, les buts sont raffinés successivement en sous-buts dans un graphe ET/OU jusqu'à être assignés à un agent. Un but assigné à un agent du système se définit comme une exigence. Un but assigné à un agent de l'environnement du système est défini comme une attente. Un sous-but participe (achieve, maintain, avoid …) de manière positive ou négative à l'accomplissement de son but parent. Tout cet ensemble permet de mener des spécifications, des analyses de risque, d'analyse d'alternatives.

Dans cette approche, il nous semble intéressant de conserver l'expressivité de la décomposition (des buts aux exigences ou aux attentes), sous la forme d'arbre ET/OU qui peuvent être utiles pour les notions de variabilité, la contribution positive ou négative, d'allocation aux agents (du système ou non).

4.3 Six questions à se poser (entre autres)

Nous avons vu que l'ingénierie des exigences était un sujet vaste, avec peu d'approches globales du sujet mais plutôt une myriade de petits domaines peu interconnectés. La métamodélisation est, quant à elle, forcément dirigée dans un but particulier. Il est nécessaire de se poser un certain nombre de questions qui vont

pouvoir nous mener des données d'entrée jusqu'à l'analyse que l'on souhaite mener. Ces questions sont proches des conseils proposés par (Yue *et al*, 2010) qui s'intéressait aux transformations pour atteindre des modèles UML.

Quels sont les objectifs à atteindre ? Un métamodèle est naturellement structuré par les objectifs qu'on lui donne, tant dans ses aspects statiques qu'opérationnels. Pourquoi chercher à modéliser les acteurs d'un projet si l'on vise la génération automatique de tests ? Inversement, pourquoi se contraindre à transformer un modèle sous la forme d'un automate si on souhaite simplement analyser un nombre d'allocation. A quel moment du projet nous situons-nous ?

Quels sont les langages en entrée de nos cas d'étude ? Les exigences sont pour la plupart des données textuelles, écrites en langage naturel, qu'il soit contraint ou non (vocabulaire déterminé, texte à trous…). Elles peuvent parfois déjà être formalisées sous la forme de scénarios, de cas d'usage, de propriétés, de règles. La traçabilité peut déjà être un facteur à prendre en compte à ce niveau.

Quelles sont les phases de preprocessing des exigences nécessaires avant la modélisation. Cette étape n'est pas la même si on parle de français brut ou d'une propriété exprimée sous la forme d'une règle ou d'une expression mathématique.

Quelle est le domaine métier de l'application ? Quelque soit le projet dans lequel on veut insérer une démarche d'ingénierie des exigences, il est forcément lié à un domaine métier qui possède son propre vocabulaire, voire dans le cadre de projets pluridisciplinaires, un vocabulaire qui peut se recouvrir avec des terminologies différentes ou diverger.

Quelle(s) technique(s) de transformation utiliser ? Les processus s'accordent bien avec une transformation vers des réseaux de Pétri mais si l'on souhaite aller vers une spécification textuelle ou de la génération de tests, une transformation à base de règles peut s'avérer plus appropriée. Comment sont faites ces transformations, manuellement ou automatiquement ?

Comment évaluer le résultat de la transformation et l'analyse résultante ? Cette question rejoint les précédentes et pose le double problème de la traçabilité et de la validité. On a souvent déjà commencé à transformer l'entrée originale avant même d'avoir pu commencer à analyser réellement. Comment prouver que deux expressions, dont l'une est la transformation de l'autre (par analyse lexicale, syntaxique, traitement de la langue …), sont sémantiquement identiques lorsque l'intitulé d'entrée est sujet (parfois volontairement) à interprétation ? Quels critères appliquer, et leur validité, pour décider par exemple de la bonne représentation d'une exigence lorsque l'on décide de la raffiner.

5. Travaux d'IDM appliqués à l'IE

Pour illustrer ce questionnement, nous avons choisi d'étudier quelques articles utilisant des métamodèles dans une des activités de l'ingénierie des exigences, qu'il s'agisse de spécifier des exigences, de relever des incohérences, ou d'aller vers la génération automatique de tests. Il s'agit ici de montrer la diversité des questions que l'ont peut se poser autour des exigences et des possibilités offertes par l'ingénierie dirigée par les modèles. Dans un second temps, nous essayons de nous positionner a priori par rapport à ces questions avec les contraintes que nous avons à savoir la sûreté de fonctionnement.

Dans (Vicente *et al*, 2007), les auteurs partent d'un canevas qui est le métamodèle d'exigences et qui va assurer la bonne construction d'une spécification d'exigences. Plutôt que de partir du texte pour le transformer pour avoir un modèle, c'est l'outil de modélisation qui va par la suite faire le chemin inverse vers la spécification textuelle. Dans (Goknil *et al*, 2008), les auteurs proposent un métamodèle cœur et un outillage pour le personnaliser afin de le transformer vers d'autres outils/langages pour une analyse ciblée. Leur cas d'étude est une personnalisation vers SysML et leur permet de détecter des relations implicites et/ou incohérentes entre exigences. Dans (Baudry *et al*, 2007), les auteurs présentent un modèle simulable d'exigences fonctionnelles. Ces exigences sont décrites à travers un langage naturel contraint et transformé en un ensemble de règles.

Les études de Goknil et Baudry montrent qu'il est possible de décrire un métamodèle relativement générique et de les enrichir par la suite pour des analyses ciblées par composition avec d'autres modèles. Les propositions de métamodèle de Vicente et Goknil sont relativement similaires et assez explicites. Les deux propositions possèdent des éléments de traçabilité des exigences pré-spécification (traçabilité des éléments qui amènent à exprimer une exigence d'une certaine façon) mais qui est relativement insuffisant par rapport à la réalité de la pré-spécification pour des programmes industriels complexes. On peut remarquer également un système de décomposition à la fois proche des approches orientées but et inspirée de SysML, standard de l'OMG (SysML, 2010). Celle de Baudry tient compte de la représentation originale sous forme de règles ce qui rend ce métamodèle bien moins naturel. Cependant, les transitions entre l'entrée textuelle et sa transformation vers ces règles et les modèles sont automatiques tandis que la première transformation entre exigences et éléments modélisés des deux autres est issue d'une démarche manuelle.

Par rapport à ces interrogations, procédons à la même démarche, pêle-mêle sur notre propre projet. Notre objectif est de modéliser et analyser des exigences de

sûreté et leur relation dans un triptyque exigence, allocation, qualification. Il nous faut également expliciter ces liens pré-spécification avec les éléments qui nous ont amené à avoir les exigences qui vont guider ces projets. Nos documents d'entrée sont les textes normatifs ainsi que les documents de spécification des systèmes. Toutes les données d'entrée sont en langue naturelle non contrainte et auront pour domaine, l'univers du contrôle commande avec ses propriétés à décrire. La traçabilité est un objectif fondamental tant en amont qu'en aval de la spécification et participe à la robustesse de la modélisation et à son évaluation.

6. Les défis

(Nuseibeh *et al 2000) The key question to ask for any modelling approach is "what is it good for?", and the answer should always be in terms of the kind of analysis and reasoning it offers.*

Notre objectif est donc de proposer un métamodèle d'exigences et son outillage qui puisse prendre en compte les dimensions identifiées précédemment sur la variabilité des exigences, des allocations et des démarches de qualification et la traçabilité pré et post spécification. Une telle représentation a pour but d'aider à s'approprier le cadre réglementaire et son côté implicite, mieux connaître les impacts des changements à travers leurs répercutions dans le système. Un autre challenge serait, à partir d'une telle approche, de faire tendre la vision par palier technologique des systèmes complexes vers celles des lignes de produit où l'on saurait être capable d'identifier un cœur générique et une partie variable, interchangeable tout en continuant à respecter les critères de sûreté imposés.

7. Conclusion

Les problématiques qui nous touchent sont à la convergence entre trois domaines d'ingénierie : le logiciel, le système et les exigences. L'ingénierie des exigences est un domaine particulièrement large et riche d'idées, d'approches, même s'il n'existe pas d'approche sur la totalité du domaine. L'ingénierie dirigée par les modèles est un courant de plus en plus important du génie logiciel et a montré son utilité tant pour le développement logiciel que pour l'ingénierie des exigences. Enfin l'ingénierie système nous donne la dimension pluridisciplinaire et industrielle de ces problématiques.

Nous avons la conviction que la vision que nous portons à travers l'ingénierie dirigée par les modèles et à travers les mécanismes de métamodélisation et de

transformation de modèles peut être utilisée pour maîtriser les impacts de la variabilité au niveau des exigences et des éléments où on les retrouve. Nous avons proposé un canevas théorique pour guider nos travaux sous la forme de six questions dont la réponse est un objectif vers lequel tendre. Si les problématiques que nous avons soulevées peuvent s'appliquer à tous les niveaux d'abstraction d'un système, nos travaux futurs se focaliseront sur la modélisation des exigences de sûreté pour le domaine du contrôle commande mais peuvent s'appliquer à tous les contextes des projets industriels complexes : dans l'automobile, dans l'avionique, l'aérospatial, tous les domaines où la sûreté de fonctionnement est un pré-requis en conception.

8. Bibliographie

Baudry B., Nébut C., Le Traon Y., « Model-driven Engineering for Requirements Analysis », *In EDOC'07 (Entreprise Distributed Object Computing Conference)*, 2007

Cheng B., Atlee J., « Research Directions in Requirements Engineering » *In IEEE ICSE 2007, Future of Software Engineering*, pp. 285-303

Goknil A., Kurtev I., Van Den Berg K., « A Metamodeling Approach for Reasoning about Requirements », *In 4th European Conference Model Driven Architecture - Foundations and Applications, ECMDA-FA 2008*, 9-13 June 2008, Berlin, Germany. pp. 310-325

Gotel O. C. Z., Finkelstein A. C. W., « An Analysis of the Requirements Traceability Problem », *In RE 1994*, IEEE Computer Society Press, Colorado Springs, Colorado USA, 18-22 April 1994

Jézéquel J.-M., Gérard S., Baudry B., « *L'ingénierie dirigée par les modèles* », chapitre « Le génie logiciel et l'IDM : une approche unificatrice par les modèles », Lavoisier, Hermes-science, 2006.

Norme IEEE 1233, édition 1998 Guide de l'IEEE pour la Spécification d'Exigences de Système

Nuseibeh B., Easterbrook S., « Requirements engineering: a roadmap », *In IEEE ICSE 2000*, pp 35–46

OMG SysML specification: *http://www.omg.org/spec/SysML/1.2/*

Van Lamsweerde A., *« Requirements Engineering. From system goals toUML Models to Software Specification »*, Wiley, 2009

Yu E., « Social Modeling and i* », *In Lecture Notes in Computer Science, 2009, Volume 5600, Conceptual Modeling: Foundations and Applications*, Pages 99-121

Yue T., Briand L., Labiche Y., « A systematic review of transformation approaches between User requirements and analysis models », *In Requirements Engineering Journal, Online First™, 25 August 2010*

Vicente-Chicote C., Moros B., Toval A., « REMM-Studio: an Integrated Model-Driven Environment for Requirements Specification, Validation and Formatting », *In Journal of Object Technology, Special Issue TOOLS EUROPE 2007*, Vol. 6, No. 9, pp. 437-454, October 2007